



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/668,112	09/22/2000	Michael L. Grandcolas	CITI0185	9577
27510	7590	04/19/2004	EXAMINER	
KILPATRICK STOCKTON LLP 607 14TH STREET, N.W. SUITE 900 WASHINGTON, DC 20005			PARTHASARATHY, PRAMILA	
			ART UNIT	PAPER NUMBER
			2136	
DATE MAILED: 04/19/2004				

8

Please find below and/or attached an Office communication concerning this application or proceeding.

PRL

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	09/668,112	GRANDCOLAS ET AL.
	<b>Examiner</b>	<b>Art Unit</b>
	Pramila Parthasarathy	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 18 June 2003.

2a) This action is FINAL.                    2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-48 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1-48 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:

1. Certified copies of the priority documents have been received.

2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.

3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date #5 and #7.	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____.

**DETAILED ACTION**

1. This action is in response to the application filed on 06/18/2003. Claims 1 – 48 were received for consideration. No preliminary amendments to the claims were filed. Claims 1 – 48 are currently being considered.

2. Two initialed and dated copies of Applicant's IDS form 1449; Paper No.5 and 7 are attached to the Office action.

***Drawings***

The drawings are objected to under 37 CFR 1.83(a) because they fail to show 100, 102 and 110 as described in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Applicant needs to label Fig.3 properly.

***Specification***

The disclosure is objected to because of the following informalities: incorrect labeling of items in the detailed description.

Website 49 should be changed to 149 on page 13 line1.

Item 70 should be changed to 170 on page 13 line19.

Item 77 should be changed to 177 on page 13 lines 6 and 14.

Item 80 should be changed to 180 on page 13 line 30 and on page 14 line 7.

Item 83 should be changed to 183 on page 13 line 29 and on page 14 line 4

Details for items 179 and 181, Fig. 4 are missing from the detailed description

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1- 48 are rejected under 35 U.S.C. 102(e) as being anticipated by Sasmazel et al. (U.S. Patent No.: 6,263,432).

Regarding Claim 1, Sasmazel teaches and describes, a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), comprising:

authenticating a user at the first web server (Fig. 5, Column 7 lines 39 – 61; Fig. 6, and Column 8 lines 1 – 45) ;

transmitting an encrypted authentication token from the first web server to a second web server, wherein the authentication token comprises an expiration time and is digitally signed by the first web server (Fig. 3, # 302; Fig.5 and Column 7 lines 39 – Column 8 line 56) ;

authenticating the authentication token at the second web server (Fig. 7 and Column 8 lines 57 – Column 9 line 9); and

allowing the user to conduct a session at the second web server (Fig. 7 and Column 9 line 10 – 30).

Regarding Claim 15, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), comprising:

allowing a user at a computing device to access a first web server in the federation of web servers via a web browser of the computing device (Fig. 2 #210 and Column 6 lines 10 – 13);

authenticating the user with user-provided authentication information, including at least a user identification, by the first web server (Fig. 5 Column 7 lines 39 – 61; Fig. 6 and Column 8 lines 1 – 45);

prompting the user for selection of a functionality offered via the second web server (Column 6 lines 10 – 27);

receiving a selection by the user of the functionality offered via the second web server (Column 6 lines 10 – 40);

creating an authentication token for the user including at least the user identification and with a pre-defined token expiry by the first web server (Fig. 3, #302; Fig.5 and Column 7 lines 39 – 61);

digitally signing the authentication token by the first web server (Fig. 3 #306 and Column 7 lines 39 – 61);

qualifying the domain attribute of the authentication token with the shared sub-domain name by the first web server (Fig. 6, Column 7 lines 39 – Column 9 line 5);

sending the digitally signed authentication token to the web browser of the computing device by the first web server (Column 7 lines 39 – Column 8 line 58);

redirecting the web browser to the second web server by the first web server (Column 6 lines 28 – 30 and Column 8 lines 56 - 58);

sending the authentication token to the second web server by the web browser (Fig. 7 and Column 8 lines 57 – Column 9 line 9);

decrypting the authentication token by the second web server (Fig.7 and Column 8 lines 57 – Column 9 line 9);

checking the pre-defined expiry of the authentication token by the second web server (Fig.7 and Column 8 lines 57 – Column 9 line 9); and

allowing the user to conduct a session with the second web server if within the pre-defined token expiry (Fig.7 Column 8 lines 57 – Column 9 line 30).

Regarding Claim 20, Sasmazel teaches and describes, a method of single sign-on for multiple web servers (Fig. 7 and Column 10 lines 10 – 30), comprising:

receiving log-in data from a user in a first server ( Fig. 5 and Column 7 lines 39 – 61; Fig. 6 and Column 8 lines 1 – 45);

providing the user with a service selector (Column 6 lines 10 – 27);

receiving an indication that the user selected the service selector (Column 6 lines 10 – 40);

constructing an authentication token comprising profile data associated with the user (Fig. 3 #302; Fig. 5 Column 7 lines 39 – 61; Fig. 6 and Column 8 lines 1 – 45);

encrypting and signing the authentication token (Fig. 3 #306 and Column 7 lines 39 – 61);

redirecting the user to a second server (Column 6 lines 28 – 30 and Column 8 lines 56 – 58);

transmitting the authentication token to the user (Column 7 lines 39 – Column 8 lines 58);

receiving the authentication token in the second server (Column 8 lines 46 – 58 and Column 10 lines 18 – 24);

verifying the authentication token in the second server (Fig. 7 and Column 8 lines 57 – Column 9 line 9); and

allowing the user access to a service provided by the second server (Fig. 7 Column 8 lines 57 – Column 9 line 30).

Regarding Claim 25, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), comprising:

a means for authenticating a user at the first web server ( Fig. 5, Column 7 lines 39 – 61; Fig. 6 and Column 8 lines 1 - 45);

a means for transmitting an encrypted authentication token from the first web server to a second web server, wherein the authentication token comprises an expiration time and is digitally signed by the first web server (Fig. 3 #302, Column 6 lines 65 – Column 7 line 61);

a means for authenticating the authentication token at the second web server (Fig. 6, 7; and Column 8 lines 57 – Column 9 line 9); and

a means for allowing the user to conduct a session at the second web server (Fig. 7 Column 8 lines 57 – Column 9 line 30).

Regarding Claim 39, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), comprising:

a means for allowing a user at a computing device to access a first web server in the federation of web servers via a web browser of the computing device (Fig. 2 #210 and Column 6 lines 10 – 13);

a means for authenticating the user with user-provided authentication information, including at least a user identification, by the first web server (Fig. 6, Column 6 lines 10 – 57 and Column 8 lines 1 – 45);

a means for prompting the user for selection of a functionality offered via the second web server (Column 6 lines 10 – 27);

a means for receiving a selection by the user of the functionality offered via the second web server (Column 6 lines 10 – 40);

a means for creating an authentication token for the user including at least the user identification and with a pre-defined token expiry by the first web server (Fig. 3, #302; Fig. 5 Column 7 lines 39 – 61);

a means for digitally signing the authentication token by the first web server (Fig. 3 #306 and Column 7 lines 39 – 61);

a means for qualifying the domain attribute of the authentication token with the shared sub-domain name by the first web server (Fig. 6, Column 7 lines 39 – Column 9 line 5);

a means for sending the digitally signed authentication token to the web browser of the computing device by the first web server (Column 7 lines 39 – Column 8 lines 58);

a means for redirecting the web browser to the second web server by the first web server (Column 6 lines 28 – 30 and Column 8 lines 56 – 58);

a means for sending the authentication token to the second web server by the web browser (Fig. 7 and Column 8 lines 57 – Column 9 line 9);

a means for decrypting the authentication token by the second web server (Fig. 7 and Column 8 lines 57 – Column 9 line 9);

a means for checking the pre-defined expiry of the authentication token by the second web server (Fig. 7 Column 8 lines 57 – Column 9 line 9; and

a means for allowing the user to conduct a session with the second web server if within the pre-defined token expiry (Fig. 7 Column 8 lines 57 – Column 9 line 30).

Regarding Claim 44, Sasmazel teaches and describes, a system of single sign-on user for multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 lines 40), comprising:

a means for receiving log-in data from a user in a first server (Fig. 7 and Column 10 lines 10 – 30);

a means for providing the user with a service selector (Column 6 lines 10 – 27);

a means for receiving an indication that the user selected the service selector (Column 6 lines 10 – 40);

a means for constructing an authentication token comprising profile data associated with the user (Fig. 3, Column 7 lines 39 - 61 and Column 8 lines 1 – 45);

a means for encrypting and signing the authentication token (Fig. 3 #306 and Column 7 lines 39 – 61);

a means for redirecting the user to a second server (Column 6 lines 28 – 30 and Column 8 lines 56 – 58);

a means for transmitting the authentication token in the second server (Column 6 lines 65 – Column 7 line 61 and Column 8 lines 57 – Column 9 line 9);

a means for receiving the authentication token in the second server (Column 8 lines 46 – 58 and Column 10 lines 18 – 24);

a means for verifying the authentication token in the second server (Fig. 7 and Column 8 lines 57 – Column 9 line 9); and

a means for allowing the user access to a service provided by the second server (Fig. 7 Column 8 lines 57 – Column 9 line 30).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the first web server and the second web server share a sub-domain (Fig. 2 #220, #240 and Column 6 lines 10 – 40 and Column 10 lines 10 – 30).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising allowing the user to conduct a session with the first web server (Fig. 2 #220 and Column 6 lines 10 – Column 9 line 15).

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Sasmazel teaches and describes, a method of single sign-on for multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the authentication token further comprises expiration time data (Fig. 3 #302 and Column 7 lines 45 – 47).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the first web server and the second web server share a sub-domain (Fig. 2 #220, #240 and Column 6 lines 10 – 40 and Column 10 lines 10 – 30).

Claim 40 is rejected as applied above in rejecting claim 39. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for allowing the user to conduct a session with the first web server (Fig. 2 #220 and Column 6 lines 10 – Column 9 line 15).

Claim 45 is rejected as applied above in rejecting claim 44. Furthermore, Sasmazel teaches and describes, a system of single sign-on user for multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 lines 40), wherein the authentication token further comprises expiration time data (Fig. 3 #302 and Column 7 lines 45 – 47).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising examining the expiration time of the authentication token at the second web server and allowing the user to conduct a session at the second web server only if the expiration time has not passed (Fig. 3 #302 and Column 9 lines 10 – 32).

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the second web server shares a sub-domain with the first web server (Fig. 2 #220, #240 and Column 6 lines 10 – 40 and Column 10 lines 10 – 30).

Claim 22 is rejected as applied above in rejecting claim 21. Furthermore, Sasmazel teaches and describes, a method of single sign-on for multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the authentication token comprises a cookie (Column 6 lines 10 – 57).

Claim 27 is rejected as applied above in rejecting claim 26. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a

means for examining the expiration time of the authentication token at the second web server (Column Fig. 3 #302; Column 7 lines 45 – 47 and Column 9 lines 10 – 17).

Claim 41 is rejected as applied above in rejecting claim 40. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the second web server shares a sub-domain with the first web server (Fig. 2 #220, #240 and Column 6 lines 10 – 40 and Column 10 lines 10 – 30).

Claim 46 is rejected as applied above in rejecting claim 45. Furthermore, Sasmazel teaches and describes, a system of single sign-on user for multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 lines 40), wherein the authentication token comprises a cookie (Column 6 lines 10 – 57).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the authentication token comprises a cookie (Column 6 lines 10 – 57).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), wherein digitally signing

the authentication token by the first web server comprising digitally signing the authentication token using public key encryption (Fig. 3 #306 Column 7 lines 18 – 54).

Claim 23 is rejected as applied above in rejecting claim 22. Furthermore, Sasmazel teaches and describes, a method of single sign-on for multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the log-in data comprises a user name and password (Fig. 6 and Column 8 lines 1 – 5).

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the authentication token comprises a cookie (Column 6 lines 10 – 57).

Claim 42 is rejected as applied above in rejecting claim 41. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the means for digitally signing the authentication token by the first web server comprising means for digitally signing the authentication token using public key encryption (Fig. 3 #306 Column 7 lines 18 – 54).

Claim 47 is rejected as applied above in rejecting claim 46. Furthermore, Sasmazel teaches and describes, a system of single sign-on user for multiple web

servers (Fig. 7 and Column 4 lines 15 – Column 10 lines 40), wherein the log-in data comprises a user name and password (Fig. 6 and Column 8 lines 1 – 5).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein transmitting the encrypted authentication token from the first web server to the second web server comprises transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server (Column 8 lines 42 – 58).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising confirming a match with the digital signature (Fig. 13, Column 6 lines 44 – Column 9 line 28).

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Sasmazel teaches and describes, a method of single sign-on for multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the log-in data comprises a user name and password (Fig. 6 and Column 8 lines 1 – 5).

Claim 29 is rejected as applied above in rejecting claim 28. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the means for transmitting the encrypted authentication token from the first web server to the second web server comprises means for transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server (Column 8 lines 42 – 58).

Claim 43 is rejected as applied above in rejecting claim 42. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for confirming a match with the digital signature (Fig. 13, Column 6 lines 44 – Column 9 line 28).

Claim 48 is rejected as applied above in rejecting claim 47. Furthermore, Sasmazel teaches and describes, a system of single sign-on user for multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 lines 40), wherein the service selector comprises a hyperlink (Fig. 7 and Column 6 lines 10 - 23).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein authenticating the user at the first web

server comprises receiving a user name and password (Fig. 6 and Column 8 lines 1 – 5).

Claim 30 is rejected as applied above in rejecting claim 29. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the means for authenticating the user at the first web server comprises receiving a user name and password (Fig. 6 and Column 8 lines 1 – 5).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein transmitting the encrypted authentication token from the first web server to a second web server comprises transmitting the authentication token from the first web server to a computer of the user; and transmitting the authentication token from the computer of the user of the second web server (Column 8 lines 42 – 58).

Claim 31 is rejected as applied above in rejecting claim 30. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein transmitting the encrypted authentication token from the first web server to a second web server comprises means for transmitting the authentication token from the first web server to a

computer of the user; and means for transmitting the authentication token from the computer of the user of the second web server (Column 8 lines 42 – 58).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the first web server and the second web server comprise a federation of web servers (Column 6 lines 10 – 40, Column 8 lines 46 – 50 and Column 10 lines 40 – 50).

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the first web server and the second web server comprise a federation of web servers (Column 6 lines 10 – 40, Column 8 lines 46 – 50 and Column 10 lines 40 – 50).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein authenticating the authentication token at the second web server comprises examining the cookie (Column 8 lines 46 – 60 and Column 9 lines 10 – 15).

Claim 33 is rejected as applied above in rejecting claim 32. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the means for authenticating the authentication token at the second web server comprises means for examining the cookie (Column 8 lines 46 – 60 and Column 9 lines 10 – 15).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising URL encoding the authentication token (Column 6 lines 10 – 23 and Column 7 lines 38 – 67).

Claim 34 is rejected as applied above in rejecting claim 33. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for URL encoding the authentication token (Column 6 lines 10 – 23 and Column 7 lines 38 – 67).

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising URL decoding the authentication token at the second web server (column 9 lines 10 – 32).

Claim 35 is rejected as applied above in rejecting claim 34. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for URL decoding the authentication token at the second web server (column 9 lines 10 – 32).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising providing a web page to the user having a service selector (Column 6 lines 10 – 40).

Claim 36 is rejected as applied above in rejecting claim 35. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising providing a web page to the user having a service selector (Column 6 lines 10 – 40).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the service selector comprises a hyperlink (Fig. 7 and Column 6 lines 10 - 23).

Claim 37 is rejected as applied above in rejecting claim 36. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the service selector comprises a hyperlink (Fig. 7 and Column 6 lines 10 - 23).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the hyperlink comprises a URL for the second web server (Column 6 lines 10 – 40).

Claim 38 is rejected as applied above in rejecting claim 37. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the hyperlink comprises a URL for the second web server (Column 6 lines 10 – 40).

### Conclusion

Any response to this action should be mailed to:  
Commissioner of Patents and Trademarks, Washington, D.C. 20231 or  
**faxed to:** (703) 872-9306 for all formal communications.  
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy  
Patent Examiner  
703-305-8912  
April 09, 2004

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100